DLT's Satellite workshop in Kyoto
In honor of Masami Ito's KIJU and Pál Dömösi's 75th birthday

ABSTRACTS OF THE TALKS

Kyoto Sangyo University
September 5-7, 2018

Contents

Equations in $\mathbf{SL(2,\mathbb{Z})}$

Dedicated to Masami Ito's KIJU and Pál Dömösi's 75th birthday

Volker Diekert

Institut für Formale Methoden der Informatik, Universität Stuttgart, Germany

Abstract. There are classical connections between Hilbert's Tenth Problem, WordEquations, and $\mathrm{SL}(2,\mathbb{Z})$. This note relates them to some recent results showing that the existential theory of $\mathrm{SL}(2,\mathbb{Z})$ is in PSPACE.

Deterministic blow-ups of nondeterministic finite automata

Galina Jirásková

[1] Institute of Computer Science, Faculty of Science, P. J. Šafárik University,
Jesenná 5, 040 01 Košice, Slovakia
jozef.jirasek@upjs.sk
[2] Mathematical Institute, Slovak Academy of Sciences,
Grešákova 6, 040 01 Košice, Slovakia
jiraskov@saske.sk

Abstract. In 1997, Iwama, Kambayashi, and Takaki stated the question of whether there always exists a minimal nondeterministic finite automaton of n states whose equivalent minimal deterministic finite automaton has m states for all integers m and n satisfying that $n \leq m \leq 2^n$. We provide a survey of the results concerning this problem. We start with an alphabet that grows exponentially with n, and show that in such a case, the question can be answered positively in an easy way. For a linear alphabet, a proof by induction gives a positive answer to the question. Finally, we consider a fixed ternary alphabet and present a solution which uses the fact that every integer can be expressed as a sum of powers of two decreased by one, assuming that the smallest power may be used twice. On the other hand, the question is answered negatively in the case of a unary alphabet. The binary case is still open, and we provide a conjecture on the form of automata covering the whole range. Our computations support our conjecture.

More properties of the Fibonacci word on an infinite alphabet

Amy Glen

Murdoch University, Perth, Australia

Abstract. The well-known *Fibonacci word* F over the binary alphabet $\{0,1\}$ is the fixed point of the morphism $\psi : 0 \mapsto 01$, $1 \mapsto 0$ given by

$$F = \lim_{n\to\infty} \psi^n(0) = 01001010010010100 1010 \cdots$$

Recently Zhang, Wen, and Wu [*Electronic J. Combinatorics* 24–2 (2017) #P2.52] introduced an interesting generalisation of this infinite word. As an alphabet they used the non-negative integers, and as a morphism they used $\phi : (2i) \mapsto (2i)\cdot(2i+1)$, $(2i+1) \mapsto (2i+2)$ to give the infinite word beginning

$$W = 012232342344523445456 \cdots$$

Some of the properties of the Fibonacci word F have parallels with those of W. For example, if we reduce the elements of the W modulo 2 we obtain F.

In this talk we consider counting the number of occurrences of squares, palindromes, and Lyndon factors in the finite words $W_n := \phi^n(0)$, whose lengths are Fibonacci numbers (analogous to the so-called *finite Fibonacci words* $F_n := \psi^n(0)$).

This is joint work with Jamie Simpson (Curtin University) and Bill Smyth (McMaster University).

Magic cube and its application to secret sharing scheme

Tomoko Adachi[1] and Xiao-Nan Lu[2]

[1] Toho University
[2] Tokyo University of Science [Campus Noda]

Abstract. A magic cube of order n is an arrangement of the n^3 integers $1, 2, \ldots, n^3$ into an $n \times n \times n$ array with the property that the sums in each row and each of the main diagonals are the same.
Secret sharing schemes is a kind of cryptography in which participants share a secret value K.
Moreover, in order to treat many secret values $K_1, K_2, ..., K_t$, multiple secret sharing schemes are proposed.
In this talk, we investigate multiple secret sharing schemes using magic cubes.

Equivalent Varieties of Multialgebras

Thawhat Changphas[1] and Panuwat Luangchaisri[1]

Department of Mathematics, Faculty of Science, Khon Kaen University, Thailand, 40002

Abstract. As in the article of S. Busaman and K. Denecke [Solidifyable Minimal Clones of Partial Operations, Automata, Formal Languages and Algebraic Systems Proceedings of AFLAS 2008, 1-21.], in this paper, we characterize when varieties of multialgebras are equivalent.

Verifying every language in constant space

Maksims Dimitrijevs[1] and Abuzer Yakaryilmaz[1]

University of Latvia

Abstract. We have been investigating the minimal resources for probabilistic machines to recognize uncountably many languages. Very recently, we focused on probabilistic verifiers by also considering the verification of every language. In this paper, we investigate the verification of every language in constant space and we present two different protocols. In the first protocol, the verifier communicates with two provers. In the second protocol, the verifier communicates with a single prover but each non-member may not be rejected with high probability.

Reversible computing and algebraic compositionality

Attila Egri-Nagy

Akita International University

Abstract. Algebraic automata theory has a clear distinction between destructive memory storage and invertible computation. Homomorphisms and more general morphic relations, by their very definitions, respect this difference: we cannot embed general transformation semigroups into permutation groups. On the other hand, computers do exist. They can be modelled as transformation semigroups, and at the same time they work on top of the reversible laws of physics. How can we reconcile this seeming contradiction? In reversible computing, this has been done several times on different models (mathematical functions, gate logic, cellular automaton, billiard balls, etc.). Here we do the same for the semigroup theoretic model of computation, with special attention for retaining the compositional nature of abstract algebra.

Clusters of distinct square roots

Szilárd Zsolt Fazekas

Akita University

Abstract. This is a report on a work in progress with the main goal of solving a decades old conjecture regarding the maximum number of distinct squares that a word can contain. We introduce a new approach to counting distinct repetitions in a word. While most previous approaches focused on counting specific positions of repetitions, such as the start of occurrences or the lexicographically minimal positions, we identify distinct squares with the set of all positions where their root occurs, called square clusters. An upper bound on the number of clusters included in another cluster, as a function of the cluster size would imply an upper bound on the number of distinct squares as a function of the word length. While not yet being able to improve the known bounds, we present some basic properties of clusters and indicate possible avenues to pursue in the future.

A new result in code-based Cryptography: a cryptosystem based on error-correcting codes ⋆ ⋆⋆

Pál Dömösi[1], Carolin Hannusch[1], and Géza Horváth[1]

University of Debrecen, Hungary
domosi@unideb.hu
hannusch.carolin@inf.unideb.hu
horvath.geza@inf.unideb.hu

Abstract. In this talk we introduce a new cryptographic system which is based on the idea of encryption due to McEliece [2]. We use the McEliece encryption system with a new linear error-correcting code, which was constructed in [1]. We show how encryption and decryption works within this cryptosystem and we give the parameters for key generation. Further, we explain why this cryptosystem is post-quantum. We will introduce a method of generating a binary $(4096, 2048, 64)$-code, which can be used in this encryption system.

References

1. Hannusch, C., and Lakatos, P.: Construction of self-dual binary $[2^{2k}, 2^{2k-1}, 2^k]$-codes, Algebra and Discrete Mathematics Vol.21 Nr.1, pp.59-68 (2016)
2. McEliece, R.J.: A Public-Key Cryptosystem Based On Algebraic Coding Theory. DSN Progress Report. 44, pp.114-116 (1978)

⋆ This work was supported by the National Research, Development and Innovation Office of Hungary under Grant No. TÉT 16-1-2016-0193

⋆⋆ This work was supported by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project was co-financed by the Hungarian Government and the European Social Fund.

The Range of State Complexities of Languages Resulting from the Cut Operation

Markus Holzer[1] and Michal Hospodár[2]

[1] Institut für Informatik, Universität Giessen
[2] Mathematical Institute, Slovak Academy of Sciences, Košice

Abstract. We investigate the state complexity of languages resulting from the cut operation of two regular languages represented by minimal deterministic finite automata with m and n states, respectively. We show that the entire range of complexities, up to the known upper bound, can be produced in the case when the input alphabet has at least two symbols. Moreover, we prove that in the unary case, only complexities up to $2m-1$ and between n and $m+n-2$ can be produced, while if $2m \leq n-1$, then the complexities from $2m$ up to $n-1$ cannot be produced.

Security Analysis of Stream Ciphers: DH3 vs. OTP

Géza Horváth

University of Debrecen, Faculty of Informatics

Abstract. In this talk we are going to show the DH3 stream cipher based on automata theory.
In the first part of the talk, we are going to show that the DH3 stream cipher is safe against known plaintext attack, and man in the middle attack, contrary to the very popular OTP stream cipher.
In the second part of the talk, we are going to prove that the DH3 stream cipher satisfies the condition of perfect secrecy.

Nondeterministic Complexity of Power and Positive Closure on Subclasses of Convex Languages

Michal Hospodár[1] and Matúš Palmovský[1]

Mathematical Institute, Slovak Academy of Sciences, Košice

Abstract. We study the nondeterministic state complexity of the k-th power and positive closure operations on the classes of prefix-, suffix-, factor-, and subword-free, -closed, and -convex regular languages, and on the classes of right, left, two-sided, and all-sided ideal languages. It is known that in the class of regular languages, the nondeterministic state complexity of these two operations is given by the functions kn and n, respectively. We show that the upper bound kn on the complexity of the k-th power is tight for closed and convex classes, while in the remaining classes, the tight upper bound is $k(n-1)+1$. Next we show that the upper bound n on the complexity of the positive closure operation is tight in all considered classes except for classes of factor-closed and subword-closed languages, where the complexity is 1. All our worst-case examples are described over a unary or binary alphabet, except for witnesses for the k-th power on subword-closed and subword-convex languages which are described over a ternary alphabet. Moreover, whenever a binary alphabet is used for describing a worst-case example, it is optimal in the sense that the upper bounds cannot be met by a language over a unary alphabet. The most interesting result is the describing of a binary factor-closed language meeting the upper bound kn for the k-th power. To get this result, we use a method which enables us to avoid tedious descriptions of fooling sets.

Syntactic Unification over Rational Terms Revisited

Munehiro Iwami

Shimane University, Japan

Abstract. Syntactic unification algorithms over rational terms have been studied in several papers. However, the discussions in such papers are not enough to clarify the relationship between the set of equations obtained by inference rules and the rational substitution that is most general unifier. Furthermore, the precise proofs of termination, soundness and completeness are not clear in many cases. In this talk, we revisit the foundations of syntactic unification algorithm over rational terms within the framework of term rewriting systems. First, we describe the relationships between the rational term, regular system and unification algorithm over rational terms. Next, we reformulate the syntactic unification algorithm over rational terms by inference rules, and then give the proofs of its termination, soundness and completeness, respectively. Finally, we prove that a set E of equations is unifiable over rational terms if and only if there exists a most general unifier of E as a rational substitution. This talk is based on our paper which will be published in Computer Software.

Deterministic Blow-ups of Binary Nondeterministic Finite Automata (work in progress)*

Jozef Jirásek[1] and Galina Jirásková[2]

[1] Institute of Computer Science, P. J. Šafárik University, Košice, Slovakia
jozef.jirasek@upjs.sk
http://ics.upjs.sk/
[2] Mathematical Institute, Slovak Academy of Sciences, Košice, Slovakia
jiraskov@saske.sk
http://im.saske.sk/∼jiraskov/

Abstract. It is known that for all m and n such that $n \leq m \leq 2^n$, there exists a minimal nondeterministic finite automaton of n states and defined over a ternary alphabet whose equivalent minimal deterministic automaton has exactly m states. On the other hand, this is not true in the case of unary alphabet where there are a lot of gaps in the range from n to 2^n that cannot be achieved by the number of states in a minimal deterministic automaton equivalent to a given minimal unary nondeterministic automata of n states. The binary case is still open. We provide a survey of partial results for the binary case showing that all values from n to $2^{n/3}$ and from $2^n - 3n$ to 2^n are achievable by deterministic blow-ups of binary nondeterministic automata. We also present a conjecture on a form of binary nondeterministic automata that cover the whole range from n to 2^n by their deterministic blow-ups. Our computations support our conjecture up to $n = 17$.

Keywords: deterministic and nondeterministic finite automata, minimal automata, binary alphabets

* Research supported by VEGA grant 1/0056/18 and grant APVV-14-0598 and APVV-15-0091.

Regular Aspects of k-Abelian Equivalence

Juhani Karhumäki[1] and Markus A. Whiteland[1]

Department of Mathematics and Statistics, University of Turku

Abstract. The topic of this presentation is a generalization of Abelian equivalence of words, which lies in between Abelian equivalence and equality of words. Let $k > 0$ be an integer. Two words u and v over alphabet A are said to be k-Abelian equivalent if, for each word x of length at most k over A, the number of occurrences of x as a factor of u is the same as for v. The k-Abelian equivalence defines an equivalence relation on A^*. For $k = 1$, the 1-Abelian equivalence coincides with the Abelian equivalence. If two words u and v are k-Abelian equivalent for all positive integers k, then u and v are equal. Further, if two words are k-Abelian equivalent, then they are t-Abelian equivalent for all $t \leq k$.

We review the research on the k-Abelian equivalence classes. We start from a characterization of k-Abelian equivalence, in terms of rewriting, which opened new aspects in the k-Abelian equivalence relation. In particular, a straightforward application of this characterization shows that the language of lexicographically least representatives of the k-Abelian equivalence classes over a fixed alphabet A is regular. Similarly the language of words x, for which the k-Abelian equivalence class represented by x is the singleton $\{x\}$, is shown to be regular. Building on these initial observations, we show that, for any fixed integer $r > 0$, the language of words x, for which the k-Abelian equivalence class represented by x has cardinality r, is regular.

We explore other language theoretic properties related to k-Abelian equivalence, and discuss implications to other notions related to k-Abelian equivalence.

This presentation is based on the works

J. Cassaigne, J. Karhumki, S. Puzynina, M.A. Whiteland: k-Abelian Equivalence and Rationality, Fundamenta Informaticae 154:1-4, pp. 65-94 (2017)

J. Karhumki, S. Puzynina, M. Rao, M.A. Whiteland: On Cardinalities of k-Abelian Equivalence Classes, Theoretical Computer Science 658:A, pp. 190-204 (2017)

J. Karhumki, M.A. Whiteland: Regularity of k-Abelian Equivalence Classes of Fixed Cardinality, submitted (2018)

The quotient of a numerical semigroup with high conductor by two or three

Jiryo Komeda

Kanagawa Institute of Technology

Abstract. A numerical semigroup H means a submonoid of the additive monoid of non-negative integers whose complement is a finite set. The cardinality of the complement is called the genus of H. The conductor c of H is the smallest integer such that any integer larger than or equal to c belongs to H. The conductor of H is less than twice the genus plus one. We construct towers of numerical semigroups with conductor larger than twice the genus minus four through dividing by two or three. We investigate the properties of numerical semigroups in the towers.

Conversions from Regular Expressions to Automata: a Taxonomy and Some Average Size Results

Nelma Moreira

University of Porto

Abstract. We present a taxonomy of several automaton constructions from standard and extended regular expressions. Automata are related by determinisation or quotients w.r.t equivalence relations. For nondeterministic automata some average size results are considered.

Reversible Turing machines in a simple reversible triangular cellular automaton

Kenichi Morita

Hiroshima University

Abstract. We give a practical method of designing configurations that simulate given reversible Turing machines (RTMs) in an extremely simple reversible cellular automaton (CA). The CA model used here is an elementary triangular partitioned CA (ETPCA). Its triangular cell has three parts each of which has two states. Thus, it is an 8-state CA, and is defined by only four local transition rules. There are 256 ETPCAs in total, and they form one of the simplest subclasses of 2D CAs. Among 256 ETPCAs, there are 36 reversible ones. Morita (2017) showed that any RTM can be embedded in a reversible non-conservative ETPCA 0347 concisely, where 0347 is an identification number in the class of ETPCAs. Here, we focus on ETPCA 0137, which is a reversible and conservative ETPCA. We show that a particular reversible logic element with 1-bit memory having an identification number 4-31 (RLEM 4-31) is directly implemented in ETPCA 0137. Using RLEM 4-31, rather than a universal reversible logic gate, we can construct a configuration that simulates a given RTM in the cellular space of ETPCA 0137 by a simple and systematic method. We also created an emulator of ETPCA 0137 on the CA simulator Golly, by which whole computing processes of the RTM can be seen.

Different Types of Search Algorithms for Rough Sets Using Barabasi-Albert and Erdős-Rényi Graphs

Dávid Nagy

University of Debrecen

Abstract. Based on the available information in many cases it can happen that two objects cannot be distinguished. If a set of data is given and in this set two objects have the same attribute values, then these two objects are called indiscernible. This indiscernibility has an effect on the membership relation, because in some cases it makes our judgment uncertain about a given object. The uncertainty appears because if something about an object is needed to be stated, then all the objects that are indiscernible from the given object must be taken into consideration. The indiscernibility relation is an equivalence relation which represents background knowledge (or its limit) embedded in an information system. In a Pawlakian system this relation is used in set approximation. Correlation clustering is a clustering technique which generates a partition using search algorithms. In the authors' previous research the possible usage of the correlation clustering in rough set theory was investigated. The result of the correlation clsutering is a partition. This partition can be understood as the system of base sets. The system gained this way has several good properties. In this work the author uses Barabasi-Albert and Erdős-Rényi graphs. The goal of this work is to show how search algorithms affect the system of base sets using these types of graphs.

On the NP-completeness of the Word Problem for Permutation Grammars

Benedek Nagy

Eastern Mediterranean University

Abstract. Formal languages and automata theory are the main fields of theoretical computer science. The main classes of the Chomsky hierarchy, the classes of regular, linear, context-free, context-sensitive and recursively enumerable languages are generated by classes of regular, linear, context-free, monotonous and phrase-structured grammars and accepted by classes of finite-state, one-turn pushdodwn, pushdown, linear bounded automata, and Turing machines, respectively. The context-free grammars (and languages) have several applications due to their generating power and nice properties. However, the world is not context-free, several phenomena of the world cannot be handled by context-free grammars. On the other hand, the context-sensitive family has some unpleasant properties and contain many very complex languages. In applications usually only some of its subsets are needed. There is a big gap between the efficiency of context- free and context-sensitive grammars, thus several branches of extensions of context-free grammars were introduced by controlling the derivations in another way, such as, for instance, priority relation among the rules In this talk we consider one of the simplest variation of permutation grammars and languages. This class of permutation grammars and languages are obtained by having productions of type $AB \to BA$ (where A, B are nonterminal symbols) in addition to context-free productions. These additional rules are called permutation rules since they allow to permute two consecutive nonterminals in the sentential form. These grammars and the generated languages were studied, e.g., in [E. Mäkinen: On Permutative Grammars Generating Context-Free Languages. BIT 25/4 (1985), 604-610.] and in [B. Nagy: Languages generated by context-free grammars extended by type AB -¿ BA rules, Journal of Automata, Languages and Combinatorics 14 (2009), 175-186.].

A brief example is shown: Let $G = (\{S, A, B, C, D\}, \{a, b, c, d\}, S, P_1 \cup P2)$, where $P_1 = \{S \to ABCD, S \to ABCDS, A \to a, B \to b, C \to c, D \to d\}$, and $P_2 = \{AB \to BA, AC \to CA, AD \to DA, BA \to AB, BC \to CB, BD \to DB, CA \to AC, CB \to BC, CD \to DC, DA \to AD, DB \to BD, DC \to CD\}$ be a permutation grammar. Obviously, the first set of rules are context-free, while in the second set there are only permutation rules. Clearly, grammar G generates the language containing exactly those words which contain the same (positive) number of a's, b's, c's and d's in any order. Thus, the example shows that the generative power of permutation grammars goes beyond context-free. These grammars can also be applied in linguistics, since in some languages, for instance, in Japanese, and in Hungarian, the word order in

a sentence is not strict, some parts of the sentences can freely be permuted. They have also close relations to descriptions and simulations of parallel processes, including shuffling, partial commutations and commutations. The class of permutation languages is properly between the class of context-free and context-sensitive languages. In this talk its parsing complexity is addressed. It is already known that it is a hard problem, since in [M. Berglund, H. Björklund, J. Björklund: Shuffled languages – Representation and recognition. Theoretical Computer Science 489-490 (2013), 1-20.], it is shown that it is NP-complete for one of its subclasses. In permutation grammars the derivations are represented by a kind of extension of derivation trees in which some of the branches may cross each other. These crossing points represent the use of permutation rules during the derivation. In the first part of the talk a non-deterministic polynomial time algorithm is shown which able to generate each word of the generated language. Based on counting the number of applied productions of various types, the complexity of the algorithm is computed. By this non-deterministic algorithm we directly show that the parsing prob- lem of the permutation languages is in the complexity class NP. That is, a polynomial upper bound of the length of the derivations is proven. On the other hand we present an NP-complete problem such that its instances can be generated by a specific permutation grammar. The 3-partition problem is a well- known NP-complete problem. Briefly it can be described as follows. Let a (multi)set M of natural numbers be given. The question is, whether one can form sets of three elements of M such that their sum is the same in a way that every elements of M is used exactly once. Already Garey and Johnson showed the NP-completeness of this problem in [M.R. Garey, D.S. Johnson: Complexity results for multiprocessor scheduling under resource constraints. SIAM Journal on Computing. 4/4 (1975), 397-411.]. This problem play important role in several NP-completeness proofs. Also, we can use it efficiently for our problem. NP-completeness of permutation grammars 3 In the presentation we show a permutation grammar with the condition that the solution of its word problem gives also the answer to a given 3-partition problem. Consequently, we have presented direct proofs to show that the language class of the permutation languages has an NP-complete parsing problem. In this way, the class of permutation languages is properly between the context-free and context-sensitive languages from complexity point of view, since these two classes has deterministic polynomial and PSPACE-complete word problem, respectively.

On Two-Sided Locally Testable Languages*

Friedrich Otto

Department of Computer Science
Faculty of Mathematics and Physics
Charles University, CZ-11800 Praha 1
otto@ktiml.mff.cuni.cz

1 Abstract

In 1971 McNaughton and Papert introduced the strictly locally testable and the locally testable languages [4]. These languages have received much attention in the literature because of their elegance and simplicity. A language L over Σ is called strictly locally testable, if it is strictly k-testable for some integer $k \geq 1$, which means that there are sets A, B, C of words of length k over Σ such that a word w of length at least k belongs to L if and only if its prefix $P_k(w)$ of length k belongs to A, its suffix $S_k(w)$ of length k belongs to B, and the set $I_k(w)$ of all its inner factors of length k is a subset of C. Thus, in order to check that a word w belongs to L, an automaton with a window of size k can be used that simply moves its window from left to right across w, memorizing all factors of length k that it encounters and verifying that the above constraints are met. For a language L on Σ to be locally testable it is required that it is k-testable for some $k \geq 1$, which means that membership of a word w of length at least k only depends on its prefix $P_k(w)$, its suffix $S_k(w)$ and its set of inner factors $I_k(w)$. In fact, the set of k-testable language is just the Boolean closure of the set of strictly k-testable languages [4].

The automaton for a (strictly) locally testable language scans its input simply from left to right, just as classical models of automata, like finite-state automata or pushdown automata. But already early on researchers were also interested in devices with the ability to scan their inputs in a more flexible way. This has been achieved in several ways, for example, by two-way head motion, more than one input head, or a combination thereof. What happens if the two-head extension is applied to the machine model for the (strictly) locally testable languages that memorizes factors of a certain length? Here it makes no sense that the heads move independently of each other, as then we would just get the intersection of two (strictly) locally testable languages, which is itself a (strictly) locally testable language. Thus, the movements of the two heads must be synchronized and the factors read concurrently must be correlated in some way. This idea has been formalized in [2], leading to the notion of two-sided strictly locally testable languages.

* Joint work with Martin Kutrib from the University of Giessen. The results of this paper have been presented at NCMA 2018 in Košice, August 21–22, 2018.

Here we extend this notion to the two-sided locally testable languages, just as the strictly locally testable languages were extended to the locally testable languages in [4]. A language L over Σ is called two-sided locally testable, if there exist an integer $k \geq 1$ and a symmetric binary relation R on Σ^k such that L is k-R-testable. This means that all words $w \in L$ of length at least k are R-symmetric, and that it only depends on the prefix $P_k(w)$, the suffix $S_k(w)$, and the set $I_k(w)$ of inner factors of length k of the word w whether w belongs to L. We will see that the k-R-testable languages have a unique representation of the form $L = F_L \cup \bigcup_{(u,v,C) \in \mathrm{triple}(L)} L_R(u,v,C)$, where F_L is a set of words of length at most $k-1$, the set $L_R(u,v,C)$ consists of all R-symmetric words w of length at least k that satisfy the conditions $P_k(w) = u$, $S_k(w) = v$, and $I_k(w) = C$, and $\mathrm{triple}(L) = \{\, (u,v,C) \mid u,v \in \Sigma^k, C \subseteq \Sigma^k \text{ such that } L_R(u,v,C) \cap L \neq \emptyset \,\}$. Based on these representations we then show that the family of k-R-testable languages is closed under the operations of union, intersection, and R-complementation, where the latter only considers R-symmetric words of length at least k. In fact, it is the closure of the strictly k-R-testable languages under these operations. Further, the family of all two-sided locally testable languages is closed under intersection and R-complementation, but it is not closed under union. Also we consider closure under the operations of reversal, concatenation, Kleene star, length-preserving homomorphisms, length-preserving inverse homomorphisms, and non-erasing inverse homomorphisms.

Concerning the expressive capacity of two-sided locally testable languages, we prove that they are contained in the even linear languages introduced in [1], extending the corresponding result on two-sided strictly locally testable languages from [2]. On the other hand, this language family is incomparable under inclusion to the regular, the deterministic linear, the deterministic context-free, and the Church-Rosser languages (see [3] for the latter). Finally, we even succeed in separating the two-sided k-testable languages from the k-testable languages by regular example languages.

References

1. V. Amar and Gianfranco R. Putzolu. On a family of linear grammars. *Inform. Control*, 7:283–291, 1964.
2. Markus Holzer, Martin Kutrib, and Friedrich Otto. Two-sided strictly locally testable languages. In Rudolf Freund, František Mráz, and Daniel Průša, editors, *Non-Classical Models of Automata and Applications (NCMA 2017)*, number 329 in books@ocg.at, pages 135–150, Vienna, 2017. Austrian Computer Society.
3. Robert McNaughton, Paliath Narendran, and Friedrich Otto. Church-Rosser Thue systems and formal languages. *J. ACM*, 35:324–344, 1988.
4. Robert McNaughton and Seymour Papert. *Counter-Free Automata*. Number 65 in Research monographs. MIT Press, 1971.

Generalized Superposition of Linear Tree Languages and Products of Linear Tree Languages

Bundit Pibaljommee[1] and Pongsakon Kitpratyakul[1]

Khon Kaen University

Abstract. A linear tree language of a given type is a set consisting of linear terms, terms containing no multiple occurrences of the same variable, of that type. Instead of the usual generalized superposition of tree languages, we define the generalized linear superposition to deal with linear tree languages and study its properties. Using this superposition, we define the product of linear tree languages. This product is not associative on the collection of all linear tree languages, but it is associative on some subsets of this collection whose products of any element in the subsets are nonempty. We attempt to classify such subsets and study properties of the obtained semigroup especially in idempotent elements, regular elements, and Green's relation $\mathcal{L}$ and $\mathcal{R}$.

A result of a student of Erdős

Chiara Bindi[1], Marco Pellegrini[2], and Giuseppe Pirillo[3]

[1] Istituto di Istruzione Secondaria Superiore "Giuseppe Peano", via Andrea del Sarto 6/A, 50135 Firenze, Italy, email: chiarabindi@profbindi.eu
[2] Liceo Classico Scientifico "XXV Aprile", via Milano 36, 56025 Pontedera (Pisa), Italy, email: m19700530@hotmail.com
[3] Dipartimento di Matematica e Informatica "Ulisse Dini", viale Morgagni 67/A, 50134 Firenze, Italy, email: pirillo@math.unifi.it

Abstract. A result of a student of Erdős is well-know: *for every integer* $n \geq 1$*, each subset of* $I(2n) = \{1, 2, \ldots, n+1, n+2, \ldots, 2n\}$ *having size* $n+1$*, contains at least two distinct elements of which the smallest divides the largest.* This is proved using the pigeonhole principle. In strict relation with this result, here we study the n-sets and improve the results of a previous paper.
Keywords: n-tuple, divisor, multiple.

The Carboncettus quasi-regular octagon and other polygons

Giuseppe Pirillo

Dipartimento di Matematica "Ulisse Dini"

Abstract. The purpose of this abstract is to announce an article in honor of Masami Ito's KIJU.

First of all, we shortly recall the results of the articles of 2017 *Some recent results of Fibonacci numbers, Fibonacci words and Sturmian words* (Southeast Asian Bull. of Math.), *La scuola pitagorica ed i numeri di Fibonacci* (Archimede), *L'origine pitagorica dei numeri di Fibonacci* (Periodico di Matematiche), *Figure geometriche su un portale del Duomo di Prato* (Prato Storia e Arte), *A characterization of Fibonacci numbers* (ArXiv) where Pirillo presented the audacious thesis that the first mathematicians that discovered the "so called" Fibonacci numbers were some members of the Pythagorean School, well documented and active in Crotone in the 6th, 5th and 4th centuries B.C.
In particular we recall here the following definition and proposition.

Definition 1. *Let β a positive integer. When there exists a positive integer α such that, for some non-negative integer γ, the equality*

$$\beta(\beta+\alpha)-\alpha^2=(-1)^\gamma$$

holds, then we say that β is a Hippasus number *and that α is a* Hippasus successor *of β.*

Proposition 1. *A positive integer is a Hippasus number if, and only if, it is a Fibonacci number.*

Pirillo proposed two proofs of this proposition, the first one uses *induction principle*, and the second one uses the *minimum principle*.

In addition to the construction of the Carboncettus quasi-regular octagon, we here present similar constructions for other quasi-regular polygons with an even number of edges.

Words Separation and Positive Identities in Symmetric Groups

Arseny Shur[1] and Olga Karpova[1]

Ural Federal University

Abstract. This is a work-in-progress report on short positive identities in finite symmetric groups. The interest to such identities is inspired by the problem of separating words with finite automata, in particular, with the automata in which all letters act on the state set as permutations.

Additive decomposition of iterative quantum search operations and its significance for quantum searches

F. Masafumi Toyama[1] and Wytse Van Dijk[2]

[1] Department of Computer Science, Kyoto Sangyo University
[2] Department of Physics, Redeemer University College, Ancaster, Ontario L0K 1J4, Canada and Department of Physics and Astronomy, McMaster University, Hamilton, Ontario, Canada L8S 4M1

Abstract. In the Grover-type quantum search process a search operator is iteratively applied on the initial database state. We present an additive decomposition scheme such that the iteration process is expressed as a linear combination of k operators, where k is the number of searches and each decomposition element consists of a single search operator of the Grover-type with an overall phase-rotation transformation. It is shown that the overall phase is the same as that introduced in the search algorithm with certainty [1]. Further, we show that the final search state can be expressed in terms of a single oracle operator and phase-rotation transformations [2].
Except for the two-dimensional case, the additively decomposed form looses the unitarity, although the norm of the search state is preserved in the search process. In the present talk, in particular we discuss how a unitary search operator can be constructed with the additive form and how it can be utilized for effectively reducing the computational load of the iterative search.

[1] F. M. Toyama, W. van Dijk, and Y. Nogami, Quant. Info. Process. 12, 1897 (2013).
[2] F. M. Toyama, W. van Dijk, Quant-ph arXiv:1706.01519 (2017).

Weak-measurement experiments on qubits of IBM Cloud Q

F. Masafumi Toyama

Department of Computer Science, Kyoto Sangyo University

Abstract. We present weak-measurement experiments on qubits of IBM Cloud Q that is a universal (gate-model) quantum computer. This experiment is based on our expectation that the dynamics of spin $\frac{1}{2}$ in a magnetic field can physically be simulated by gate operations on the superconducting qubits of the transmon type.

The weak measurement is known to be a way to explore the weak values that are defined in terms of the normal time-evolution of a pre-selected state and the reversed time-evolution of a post-selected state. The notion of the weak value originates in time-symmetric interpretation of quantum mechanics. We generate time-evolutions of the qubit- states (spin-states) by making use of Grover's quantum-search operators. We construct the time-evolution models such that they give rise to quantum entanglements between the two-qubit states in their normal and reversed time-evolutions. With the time-evolution models we extract weak-values of tensor-products $\sigma_i \otimes \sigma_i (i = x, y, z)$ that correspond to tensor-product of spin $\frac{1}{2}$.

Although the experiment we propose experimentally tests the time symmetric interpretation of quantum mechanics, it also tests the ro bustness of IBM's superconducting qubits. In this talk we present our basic idea and the preliminary experimental results.

Slowly Synchronizing Automata with Idempotent Letters of Low Rank

Mikhail Volkov

Ural Federal University [Ekaterinburg]

Abstract. We use a semigroup-theoretic construction by Peter Higgins in order to produce, for each even n, an n-state and 3-letter synchronizing automaton with the following two features: 1) all its input letters act as idempotent selfmaps of rank at most $\frac{n}{2}$; 2) its reset threshold is asymptotically equal to $\frac{n^2}{2}$.